

L'AI generativa e la cybersecurity, un'arma a doppio taglio per le aziende globali. Il Rapporto

SCARICA IL REPORT "NEW DEFENSES, NEW THREATS: WHAT AI AND GEN AI BRING TO CYBERSECURITY"

AI, gen AI e cybersecurity, la situazione delle nostre imprese

La rapida diffusione dell'intelligenza artificiale (AI) e dell'AI generativa (Gen AI) sta trasformando il panorama della **cybersecurity** globale. Secondo il nuovo rapporto di Capgemini Research Institute, *"New defenses, new threats: what AI and gen AI bring to cybersecurity"*, il **97% delle organizzazioni intervistate ha riscontrato violazioni o problemi di sicurezza legati all'uso della Gen AI** nell'ultimo anno.

Nonostante i rischi emergenti, però, queste tecnologie offrono comunque strumenti senza precedenti per rafforzare la difesa contro attacchi sempre più sofisticati. Il problema è saperli gestire nel migliore dei modi, raggiungendo il potenziale massimo e tenendo sempre in massima considerazione la sicurezza.

Rischi crescenti, l'altra faccia

della medaglia dell'AI generativa

Le organizzazioni stanno sperimentando nuove vulnerabilità a causa della crescente adozione della Gen AI:

- **Il 67%** delle aziende teme fughe di dati sensibili o l'inquinamento dei dataset utilizzati per addestrare i modelli di AI.
- **I deepfake** hanno generato perdite finanziarie per oltre il **43%** delle imprese.
- Settori come automotive (78%) e consumer (70%) sono particolarmente preoccupati per l'alterazione dei dati, mentre il **75%** delle società bancarie teme il furto di proprietà intellettuale attraverso i dataset di addestramento.

Le violazioni dei dati sono costate tra **50 e 100 milioni di dollari** al **61% delle aziende bancarie** e al **62% delle organizzazioni pubbliche**.

AI come strumento di difesa proattiva

Nonostante i rischi, l'AI è diventata una tecnologia strategica per la cybersecurity. Oltre il **76%** delle organizzazioni la utilizza per migliorare la sicurezza dei dati, con percentuali che raggiungono l'**85%** nei settori banking e aerospaziale/difesa (A&D).

I vantaggi principali includono:

- Riduzione del **time-to-detect**: più del **60%** delle aziende ha ridotto i tempi di rilevamento degli attacchi di almeno il 5%.
- Accelerazione del ripristino: quasi il **40%** ha diminuito i tempi di recupero grazie all'AI.
- Miglioramento delle strategie di difesa proattive: il

61% delle aziende considera l'AI essenziale per anticipare e neutralizzare minacce complesse.

Settori in prima linea

Industrie come automotive (68%), banking (66%) e retail (63%) stanno aumentando i budget destinati alla cybersecurity. Le aziende high-tech (65%) si stanno focalizzando su tecnologie avanzate per proteggere infrastrutture critiche e dati sensibili.

L'adozione dell'AI consente agli analisti di cybersecurity di concentrarsi su minacce più sofisticate, lasciando alla tecnologia il compito di monitorare e rispondere alle minacce quotidiane.

Un futuro di opportunità e sfide

Secondo **Monia Ferrari**, Amministratore Delegato di Capgemini Italia, *“L'AI e la Gen AI rappresentano un'arma a doppio taglio. Se da un lato introducono rischi senza precedenti, dall'altro offrono strumenti innovativi per limitare gli incidenti e trasformare le strategie di difesa.”*

Per trarre pieno vantaggio da queste tecnologie, Ferrari sottolinea l'importanza di:

- Monitoraggio continuo delle minacce.
- Creazione di solide infrastrutture di gestione dei dati.
- Formazione del personale per sensibilizzarlo sui rischi dell'uso improprio dell'AI.

In un contesto di minacce in rapida evoluzione, l'intelligenza artificiale sta emergendo non solo come un punto critico di vulnerabilità, ma anche come un alleato fondamentale per garantire la sicurezza aziendale e ridurre i rischi finanziari.

Leggi le altre notizie sull'home page di Key4biz

<https://www.key4biz.it/lai-generativa-e-la-cybersecurity-unarma-a-doppio-taglio-per-le-aziende-globali-il-rapporto/515446/>